barrier designed to prevent unauthorized access (physical, audio, and visual) into these areas.

(2) Controls must be established to prevent unauthorized access to and removal of classified matter.

(3) Access to classified matter must be limited to persons who possess appropriate access authorization or other written CSA disclosure authorization and who require access in the performance of their official duties or regulatory obligations.

(4) Persons without appropriate access authorization for the area visited must be escorted by an appropriate CSA access authorized person at all times while within Restricted or Closed Areas.

(5) Each individual authorized to enter a Restricted or Closed Area must be issued a distinctive form of identification (e.g., badge) when the number of employees assigned to the area exceeds thirty per shift.

(6) During nonworking hours, admittance must be controlled by protective personnel. Protective personnel shall conduct patrols during nonworking hours at least every 8 hours and more frequently if necessary to maintain a commensurate level of protection. Entrances must be continuously monitored by protective personnel or by an approved alarm system.

(c) Due to the size and nature of the classified material, or operational necessity, it may be necessary to construct Closed Areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed Areas must be approved by the CSA. The following measures apply to Closed Areas:

(1) Access to Closed Areas must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared employee or by a CSA approved access control device or system.

(2) Access must be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified matter within the area. Persons without the appropriate level of clearance and/or need-to-know must be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented.

(3) The Closed Area must be accorded supplemental protection during nonworking hours. During these hours, admittance to the area must be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. However, doors secured from the inside with a panic bolt (for example, actuated by a panic bar), a dead bolt, a rigid wood or metal bar, or other means approved by the CSA, do not require additional locking devices.

(4) Open shelf or bin storage of classified matter in Closed Areas requires CSA approval. Only areas protected by an approved intrusion detection system will qualify for approval.

[62 FR 17693, Apr. 11, 1997, as amended at 64 FR 15652, Apr. 1, 1999]

§ 95.31 Protective personnel.

Whenever protective personnel are used to protect classified information they shall:

(a) Possess an ''L'' access authorization (or CSA equivalent) if the licensee, certificate holder, or other person possesses information classified Confidential National Security Information, Confidential Restricted Data or Secret National Security Information.

(b) Possess a ''Q'' access authorization (or CSA equivalent) if the licensee, certificate holder, or other person possesses Secret Restricted Data related to nuclear weapons design, manufacturing and vulnerability information; and certain particularly sensitive Naval Nuclear Propulsion Program information (e.g., fuel manufacturing technology) and the protective personnel require access as part of their regular duties.

[72 FR 49562, Aug. 28, 2007]

§ 95.33 Security education.

All cleared employees must be provided with security training and briefings commensurate with their involvement with classified information. The facility official(s) responsible for the program shall determine the means and methods for providing security

education and training. A licensee or other entity subject to part 95 may obtain defensive security, threat awareness, and other education and training information and material from their Cognizant Security Agency (CSA) or other appropriate sources.

(a) *Facility Security Officer training.* Licensees or other entities subject to part 95 are responsible for ensuring that the Facility Security Officer, and other personnel performing security duties, complete security training deemed appropriate by the CSA. Training requirements must be based on the facility's involvement with classified information and may include a Facility Security Officer Orientation Course and, for Facility Security Officers at facilities with safeguarding capability, a Facility Security Officer Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of Facility Security Officer.

(b) *Government-provided briefings.* The CSA is responsible for providing initial security briefings to the Facility Security Officer, and for ensuring that other briefings required for special categories of information are provided.

(c) *Temporary help suppliers.* A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, is responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using licensee's, certificate holder's, or other person's facility may conduct these briefings.

(d) *Classified Information Nondisclosure Agreement (SF–312).* The SF–312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial access authorization must, in accordance with the requirements of § 25.23 of this chapter, execute an SF–312 before being granted access to classified information. The Facility Security Officer shall forward the executed SF–312 to the CSA for retention. If the employee refuses to execute the SF–312, the licensee or other facility shall deny the employee access to classified information and submit a report to the CSA. The SF–312 must be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date.

(e) *Access to classified information.* Employees may have access to classified information only if:

(1) A favorable determination of eligibility for access has been made with respect to such employee by the CSA;

(2) The employee has signed an approved non-disclosure agreement; and

(3) The employee has a need-to-know the information.

(f) *Initial security briefings.* Initial training shall be provided to every employee who has met the standards for access to classified information in accordance with paragraph (e) of this section before the employee is granted access to classified information. The initial training shall include the following topics:

(1) A Threat Awareness Briefing;

(2) A Defensive Security Briefing;

(3) An overview of the security classification system;

(4) Employee reporting obligations and requirements; and

(5) Security procedures and duties applicable to the employee's job.

(g) *Refresher briefings.* The licensee or other entities subject to part 95 shall conduct refresher briefings for all cleared employees at least annually. As a minimum, the refresher briefing must reinforce the information provided during the initial briefing and inform employees of appropriate changes in security regulations. This requirement may be satisfied by use of audio/video materials and/or by issuing written materials to cleared employees.

(h) Persons who apply derivative classification markings shall receive training specific to the proper application of the derivative classification principles of Executive Order 13526, *Classified National Security Information* (75 FR 707; January 5, 2010), before derivatively classifying information and at least once every 2 years thereafter.

(i) *Debriefings.* Licensee and other facilities shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's access authorization is terminated, suspended, or revoked; and upon termination of the Facility Clearance.

(j) Records reflecting an individual's initial and refresher security orientations and security termination must be maintained for 3 years after termination of the individual's access authorization.

[78 FR 48041, Aug. 7, 2013]

§ 95.34 Control of visitors.

(a) *Uncleared visitors.* Licensees, certificate holders, or other persons subject to this part shall take measures to preclude access to classified information by uncleared visitors.

(b) *Foreign visitors.* Licensees, certificate holders, or other persons subject to this part shall take measures as may be necessary to preclude access to classified information by foreign visitors. The licensee, certificate holder, or other person shall retain records of visits for 5 years beyond the date of the visit.

[72 FR 49563, Aug. 28, 2007]

CONTROL OF INFORMATION

§ 95.35 Access to matter classified as National Security Information and Restricted Data.

(a) Except as the Commission may authorize, no licensee, certificate holder or other person subject to the regulations in this part may receive or may permit any other licensee, certificate holder, or other person to have access to matter revealing Secret or Confidential National Security Information or Restricted Data unless the individual has:

(1)(i) A ''Q'' access authorization which permits access to matter classified as Secret and Confidential Restricted Data or Secret and Confidential National Security Information which includes intelligence information, CRYPTO (*i.e.*, cryptographic information) or other classified communications security (COMSEC) information, or

(ii) An ''L'' access authorization which permits access to matter classified as Confidential Restricted Data and Secret and Confidential National Security Information other than that noted in paragraph (a)(1)(i) of this section except that access to certain Confidential COMSEC information is permitted as authorized by a National Communications Security Committee waiver dated February 14, 1984.

(2) An established ''need-to-know'' for the matter (See Definitions, § 95.5).

(3) NRC-approved storage facilities if classified documents or material are to be transmitted to the licensee, certificate holder, or other person.

(b) Matter classified as National Security Information or Restricted Data shall not be released by a licensee or other person subject to part 95 to any personnel other than properly access authorized Commission licensee employees, or other individuals authorized access by the Commission.

(c) Access to matter which is National Security Information at NRC-licensed facilities or NRC-certified facilities by authorized representatives of IAEA is permitted in accordance with § 95.36.

[59 FR 48975, Sept. 23, 1994, as amended at 72 FR 49563, Aug. 28, 2007]

§ 95.36 Access by representatives of the International Atomic Energy Agency or by participants in other international agreements.

(a) Based upon written disclosure authorization from the NRC Office of Nuclear Material Safety and Safeguards that an individual is an authorized representative of the International Atomic Energy Agency (IAEA) or other international organization and that the individual is authorized to make visits under an established agreement with the United States Government, an applicant, licensee, certificate holder, or other person subject to this part shall permit the individual (upon presentation of the credentials specified in § 75.8(c) of this chapter and any other credentials identified in the disclosure authorization) to have access to matter classified as National Security Information that is relevant to the conduct of a visit or inspection. A disclosure authorization under this section does not authorize a licensee, certificate holder, or other person subject to this part to provide access to Restricted Data.

(b) For purposes of this section, classified National Security Information is relevant to the conduct of a visit or inspection if—